

## REMARKS

### Amendments to the claims

Independent claim 1 has been amended to recite first means, operative in the course of said handshake, *"to pass to said peer security entity a first indication in the form of explicit information about what services are required by the local application entity"*. This amendment is based on the specification, (in particular page 14 lines 26-30), which recites that the message passed from the local application entity (Alice) includes explicit information (QRYA) reciting the services required by the local application entity, for example a set of resource operations the local application entity plans to call in the future.

Further, claim 1 has been amended to recite that the first means are operative "to receive back from said peer security entity a second indication explicitly advising what specific attributes are required of the local application entity by the remote application entity for carrying out said services" and *"to select on the basis of said second indication first attribute justifications in the form of one or more certificates from a set of available attribute justifications, and to pass the selected first attribute justifications to said peer security entity"*. This amendment is based on the specification, (in particular page 14, lines 25-26 and 30-31), which recites that the remote application entity (Bob) explicitly informs the local application entity (Alice) of what attributes are required for the services requested. The local application entity (Alice) can then select which attribute justifications to send (JUSTA).

Further, claim 1 has been amended to recite "second means, operative in the course of said handshake, to pass to said peer security entity a third indication explicitly advising what specific attributes are required of the remote application entity by the local application entity". This amendment is based on the specification (in particular page 14, lines 14-15), which recites that the local application entity (Alice) explicitly advises (in ADVB) the remote application entity (Bob) what attributes should be sent back (in JUSTB).

Independent claims 13, 20 and 22 have been amended consistently with independent claim 1. Typographical errors have been corrected in dependent claims 4 and 8. No new matter has been added.

Rejection under 35 U.S.C §102

Claims 1, 2, 4, 5 and 7-22 stand rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,643,701 to Aziz. Applicants respectfully disagree.

Claim 1

Aziz discloses (column 1, line 65 to column 2, line 5) a local application entity (client 100) calling a remote application entity (server 120). Aziz further discloses (column 2, lines 10-15) that the remote application entity 120 may use an application specific authentication to authenticate the local application entity 100, for example by asking the local application entity 100 to "supply an authentication token, such as a password, known to the server". In Aziz, if the remote application entity 120 provides a specific set of services, the local application entity 100 can call the remote application entity 120 to gain access to this specific set of services. The remote application entity 120 may then use an authentication application, specific to the remote application entity 120, to authenticate the local application entity 100. If the specific set of services includes some sensitive services (such as banking services, column 2, lines 7-9), the authentication application specific to the remote application entity 120 will consistently require high security attribute justifications from the local application entity 100. Conversely, if the specific set of services comprises only non-sensitive services, the authentication application specific to the remote application entity 120 may require low security attribute justifications from the local application entity 100 (or no justifications at all, if no authentication of the local application entity 100 is performed).

The system of Aziz allows no flexibility. If one considers an exemplary remote application entity 120 that provides both sensitive services requiring high security attribute justifications and non-sensitive services requiring low security attribute justifications, a local application entity needs to provide the high security attribute justifications to gain access to any of the services provided by the remote application

entity 120. In particular, a local application entity will need to provide the high security attribute justifications even if it only uses the non-sensitive services provided by the remote application entity 120. Consequently, in the system of Aziz, a local application entity 100 that is unable to provide the high security attribute justifications cannot gain access to the non-sensitive services provided by the remote application entity 120 above.

Applicants will now show that the features recited in claim 1 provide for a system that is more flexible than the system of Aziz. Claim 1 as amended recites that the local application entity is provided to *"pass a first indication in the form of explicit information about what services are required by the local application entity"*, to receive back *"a second indication explicitly advising what specific attributes are required of the local application entity by the remote application entity for carrying out said services, to select on the basis of said second indication first attribute justifications in the form of one or more certificates from a set of available attribute justifications, and to pass the selected first attribute justifications"*.

Considering the exemplary remote application entity above, which provides both sensitive services requiring high security attribute justifications, and non-sensitive services requiring low security attribute justifications, the system recited in claim 1 allows a local application entity that only requests access to the non-sensitive services, to pass to the remote application entity a first indication explicitly reciting only the non-sensitive services. In response, the remote application would send to the local application entity a second indication explicitly reciting only the low security attribute justifications required for carrying out the non-sensitive services, and the local application entity could, on the basis of this second indication, select the low security attribute justifications to send to the remote application entity. Consequently, in a system as recited in claim 1, a local application entity that is not able to provide the high security attribute justifications can still gain access to the non-sensitive services of the exemplary remote application entity.

Applicants submit that at least in view of the above, Aziz cannot be deemed to anticipate claim 1. Applicants further submit that Aziz does not disclose or suggest improving the flexibility of its system, in particular by introducing *"first means, operative in the course of said handshake, to pass to said peer security entity a first indication in the form*

*of explicit information about what services are required by the local application entity, to receive back from said peer security entity a second indication explicitly advising what specific attributes are required of the local application entity by the remote application entity for carrying out said services, to select on the basis of said second indication first attribute justifications in the form of one or more certificates from a set of available attribute justifications", as recited in amended claim 1. Applicants therefore submit that claim 1 is patentable over Aziz. Should the Examiner disagree, Applicants respectfully request the Examiner to clearly and specifically point out where Aziz discloses the above features, in accordance with 37 C.F.R. 1.104(c)(2).*

### Claim 13

The above arguments can be used to show that Aziz fails to disclose or suggest a method as recited in claim 13 as amended, and in particular involving "passing from the local security entity to the remote security entity a first indication in the form of explicit information about what services are required by the local system, passing from the remote security entity to the local security entity a second indication explicitly advising what specific attributes are required of the local system by the remote system for carrying out said services, selecting on the basis of said second indication first attribute justifications from a set of available attribute justifications and passing from the local security entity to the remote security entity the selected first attribute justifications in the form of one or more certificates, and passing from the local security entity to the remote security entity a third indication explicitly advising what specific attributes are required of the remote system by the local system". Applicants therefore respectfully submit that claim 13 is patentable over Aziz.

### Claims 20 and 22

The above arguments can be used to show that Aziz fails to disclose or suggest a method as recited in claim 20 as amended, and in particular involving "the local security entity explicitly indicating to the remote security entity the services and specific attributes required of said remote system by the local system, the remote security entity explicitly indicating to the local security entity the specific attributes that the remote system requires of the local system in respect of said services, and the exchange of attribute justifications, in the form of

*certificates, between the security entities, wherein the attribute justifications passed from the local security entity to the remote security entity are chosen from a set of available attributes justifications, on the basis of the explicit indication of the specific attributes that the remote system requires of the local system", or a system as recited in claim 22 as amended, and in particular comprising handshake means for effecting a security protocol handshake, "the handshake comprising the steps of (a) the local security entity explicitly indicating to the remote security entity the services and specific attributes required of said remote system by the local system, (b) the remote security entity explicitly indicating to the local security entity the specific attributes that the remote system requires of the local system in respect of said services, and (c) the exchange of attribute justifications, in the form of certificates, between the security entities, wherein the attribute justifications passed from the local security entity to the remote security entity are chosen from a set of available attributes justifications, on the basis of the explicit indication of the specific attributes that the remote system requires of the local system". Applicants therefore respectfully submit that claims 20 and 22 are patentable over Aziz.*

Claims 2, 4, 5, 7-12, 14-19 and 21

Claims 2, 4, 5 and 7-12 depend directly or indirectly on claim 1; claims 14-19 depend directly or indirectly on claim 13; and claim 21 depends directly on claim 20. Applicants submit that at least in view of their respective dependencies on claims 1, 13 or 20, claims 2, 4, 5, 7-12, 14-19 and 21 are patentable over Aziz.

In view of the above, Applicants submit that the application is now in condition for allowance and respectfully urge the Examiner to pass this case to issue.

The Commissioner is authorized to charge any additional fees that may be required or credit overpayment to deposit account no. 08-2025. In particular, if this response is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being deposited with the United States Post Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

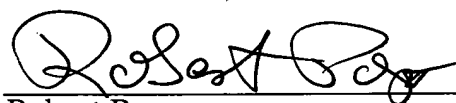
April 5, 2005  
\_\_\_\_\_  
(Date of Transmission)

Corinda Humphrey  
\_\_\_\_\_  
(Name of Person Transmitting)

  
\_\_\_\_\_  
(Signature)

April 5, 2005  
\_\_\_\_\_  
(Date)

Respectfully submitted,



Robert Popa  
Attorney for Applicants  
Reg. No. 43,010  
LADAS & PARRY  
5670 Wilshire Boulevard, Suite 2100  
Los Angeles, California 90036  
(323) 934-2300 voice  
(323) 934-0202 facsimile  
rpopa@ladasparry.com